Real-World Cryptography

David Wong

MANNING

Real-World Cryptography

Real-World Cryptography

DAVID WONG

MANNING
SHELTER ISLAND

For online information and ordering of this and other Manning books, please visit www.manning.com. The publisher offers discounts on this book when ordered in quantity. For more information, please contact

Special Sales Department
Manning Publications Co.
20 Baldwin Road
PO Box 761
Shelter Island, NY 11964
Email: orders@manning.com

Manning Publications Co.
20 Baldwin Road
PO Box 761
Shelter Island, NY 11964

Development editor: Marina Michaels
Technical development editor: Sam Zaydel
Review editor: Mihaela Batinic
Production editor: Andy Marinkovich
Copy editor: Frances Buran
Proofreader: Keri Hales
Technical proofreader: Michal Rutka
Typesetter: Dennis Dalinnik
Cover designer: Marija Tudor

ISBN: 9781617296710
Printed in the United States of America

To my parents, Anne Cerclet and Henry Wong, who nurtured curiosity in me.
To my wife, Felicia Lupu, who supported me throughout this journey.

contents

preface

As you've picked up this book, you might be wondering, why another book on cryptography? Or even, why should I read this book? To answer this, you have to understand when it all started.

A book, years in the making

Today, if you want to learn about almost anything, you Google it, or Bing it, or Baidu it—you get the idea. Yet, for cryptography, and depending on what you're looking for, resources can be quite lacking. This is something I ran into a long time ago and which has been a continuous source of frustration since then.

Back when I was in school, I had to implement a differential power analysis attack for a class. This attack was a breakthrough in cryptanalysis at that time, as it was the first side-channel attack to be published. A differential power analysis attack is something magical: by measuring the power consumption of a device while it encrypts or decrypts something, you're able to extract its secrets. I realized that great papers could convey great ideas, while putting little effort in clarity and intelligibility. I remember banging my head against the wall trying to figure out what the author was trying to say. Worse, I couldn't find good online resources that explained the paper. So I banged my head a wee more, and finally I got it. And then, I thought, maybe I could help others like me who will have to go through this ordeal.

Motivated, I drew some diagrams, animated them, and recorded myself going over them. That was my first YouTube video on cryptography: https://www.youtube.com/watch?v=gbqNCgVcXsM.

Years later, after I uploaded the video, I still receive praises from random people on the internet. Just yesterday, as I'm writing this preface, someone posted, "Thank you, really a great explanation that probably saved me hours of trying to understand that paper."

What a reward! This baby step in adventuring myself on the other side of the educational landscape was enough to make me want to do more. I started recording more of these videos, and then I started a blog to write about cryptography. You can check it out here: https://cryptologie.net.

Before starting this book, I had amassed nearly 500 articles explaining the many concepts that stand beyond this intro. This was all just practice. In the back of my mind, the idea of writing a book was slowly maturing years before Manning Publications would reach out to me with a book proposal.

The real-world cryptographer curriculum

I finished my bachelor's in theoretical mathematics and didn't know what was next for me. I had also been programming my whole life, and I wanted to reconcile the two. Naturally, I became curious about cryptography, which seemed to have the best of both worlds, and started reading the different books at my disposal. I quickly discovered my life's calling.

Some things were annoying, though: in particular, the long introductions that would start with history; I was only interested in the technicalities and always had been. I swore to myself, if I ever wrote a book about cryptography, I would not write a single line on Vigenère ciphers, Caesar ciphers, and other vestiges of history. And so, after obtaining a master of cryptography at the University of Bordeaux, I thought I was ready for the real world. Little did I know.

I believed that my degree was enough, but my education lacked a lot about the real-world protocols I was about to attack. I had spent a lot of time learning about the mathematics of elliptic curves but nothing about how these were used in cryptographic algorithms. I had learned about LFSRs, and ElGamal, and DES, and a series of other cryptographic primitives that I would never see again.

When I started working in the industry at Matasano, which then became NCC Group, my first gig was to audit OpenSSL, the most popular SSL/TLS implementation—the code that basically encrypted the whole internet. Oh boy, did it hurt my brain. I remember coming back home every day with a strong headache. What a trainwreck of a library and a protocol! I had no idea at the time that I would, years later, become a coauthor of TLS 1.3, the latest version of the protocol.

But, at that point, I was already thinking, "This is what I should have learned in school. The knowledge I'm gaining now is what would have been useful to prepare me for the real world!" After all, I was now a specialized security practitioner in cryptography. I was reviewing real-world cryptographic applications. I was doing the job that one would wish they had after finishing a cryptography degree. I implemented, verified, used, and advised on what cryptographic algorithms to use. This is the reason

I'm the first reader of the book I'm writing. This is what I would have written to my past self in order to prepare him for the real world.

Where most of the bugs are

My consulting job led me to audit many real-world cryptographic applications such as OpenSSL, the encrypted backup system of Google, the TLS 1.3 implementation of Cloudflare, the certificate authority protocol of Let's Encrypt, the sapling protocol of the Zcash cryptocurrency, the threshold proxy re-encryption scheme of NuCypher, and dozens of other real-world cryptographic applications that I unfortunately cannot mention publicly.

Early in my job, I was tasked to audit the custom protocol a well-known corporation had written to encrypt their communications. It turns out that it was using signatures on almost everything but the ephemeral keys, which completely broke the whole protocol as one could have easily replaced those—a rookie mistake from anyone with some experience with secure transport protocols, but something that was missed by people who thought they were experienced enough to roll their own crypto. I remember explaining the vulnerability at the end of the engagement and a room full of engineers turning silent for a good 30 seconds.

This story repeated itself many times during my career. There was a time when, while auditing a cryptocurrency for another client, I found a way to forge transactions from already existing ones, due to some ambiguity of what was being signed. Looking at TLS implementations for another client, I found some subtle ways to break an RSA implementation, which in turn, transformed into a white paper with one of the inventors of RSA, leading to a number of Common Vulnerabilities and Exposures (CVEs) reported to a dozen of open source projects. More recently, while reading about the newer Matrix chat protocol as part of writing my book, I realized that their authentication protocol was broken, leading to a break of their end-to-end encryption. There are so many details that can, unfortunately, collapse under you when making use of cryptography. At this point, I knew I had to write something about these. This is why my book contains many of these anecdotes.

As part of the job, I would review cryptography libraries and applications in a multitude of programming languages. I discovered bugs (for example, CVE-2016-3959 in Golang's standard library), I researched ways that libraries could fool you into misusing those (for example, my paper "How to Backdoor Diffie-Hellman"), and I advised on what libraries to use. Developers never knew what library to use, and I always found the answer to be tricky.

I went on to invent the Disco protocol (https://discocrypto.com; https://embeddeddisco.com) and wrote its fully-featured cryptographic library in less than 1,000 lines of code, and that, in several languages. Disco only relied on two cryptographic primitives: the permutation of SHA-3 and Curve25519. Yes, from only those two things implemented in 1,000 lines of code, a developer could do any type of authenticated key exchange, signatures, encryption, MACs, hashing, key derivation, and so

on. This gave me a unique perspective as to what a good cryptography library was supposed to be.

I wanted my book to contain these kinds of practical insights. So naturally, the different chapters contain examples on how to apply "crypto" in different programming languages, using well-respected cryptographic libraries.

A need for a new book?

As I was giving one of my annual cryptography training sessions at Black Hat (a well-known security conference), one student came to me and asked if I could recommend a good book or online course on cryptography. I remember advising the student to read a book from Boneh and Shoup and to attend Cryptography I from Boneh on Coursera. (I also recommend both of these resources at the end of this book.)

The student told me, "Ah, I tried, it's too theoretical!" This answer stayed with me. I disagreed at first, but slowly realized that they were right. Most of the resources are pretty heavy in math, and most developers interacting with cryptography don't want to deal with math. What else was there for them?

The other two somewhat-respected resources at the time were *Applied Cryptography* and *Cryptography Engineering* (both books by Bruce Schneier). But these books were starting to be quite outdated. *Applied Cryptography* spent four chapters on block ciphers with a whole chapter on cipher modes of operation but none on authenticated encryption. The more recent *Cryptography Engineering* had a single mention of elliptic curve cryptography in a footnote. On the other hand, many of my videos or blog posts were becoming good primary references for some cryptographic concepts. I knew I could do something special.

Gradually, many of my students started becoming interested in cryptocurrencies, asking more and more questions on the subject. At the same time, I started to audit more and more cryptocurrency applications. I later moved to a job at Facebook to lead security for the Libra cryptocurrency (now known as Diem). Cryptocurrency was, at that time, one of the hottest fields to work in, mixing a multitude of extremely interesting cryptographic primitives that so far had seen little-to-no real-world use (zero knowledge proofs, aggregated signatures, threshold cryptography, multi-party computations, consensus protocols, cryptographic accumulators, verifiable random functions, verifiable delay functions, . . . the list goes on). And yet, no cryptography book included a chapter on cryptocurrencies. I was now in a unique position.

I knew I could write something that would tell students, developers, consultants, security engineers, and others what modern applied cryptography was all about. This was going to be a book with few formulas but filled with many diagrams. This was going to be a book with little history but filled with modern stories about cryptographic failures that I had witnessed for real. This was going to be a book with little about legacy algorithms but filled with cryptography that I've personally seen being used at scale: TLS, the Noise protocol framework, the Signal protocol, cryptocurrencies, HSMs, threshold cryptography, and so on. This was going to be a book with little

theoretical cryptography but filled with what could become relevant: password-authentication key exchanges, zero-knowledge proofs, post-quantum cryptography, and so on.

When Manning Publications reached out to me in 2018, asking if I wanted to write a book on cryptography, I already knew the answer. I already knew what I wanted to write. I had just been waiting for someone to give me the opportunity and the excuse to spend my time writing the book I had in mind. Coincidentally, Manning has a series of "real-world" books, and so naturally, I suggested that my book extend it. What you have in front of you is the result of more than two years of hard work and much love. I hope you like it.

acknowledgments

Thank you to Marina Michaels for her continued help and insights and without whom this book probably wouldn't have come to completion.

Thank you to Frances Buran, Sam Zaydel, Michael Rosenberg, Pascal Knecht, Seth David Schoen, Eyal Ronen, Saralynn Chick, Robert Seacord, Eloi Manuel, Rob Wood, Hunter Monk, Jean-Christophe Forest, Liviu Bartha, Mattia Reggiani, Olivier Guerra, Andrey Labunov, Carl Littke, Yan Ivnitskiy, Keller Fuchs, Roman Zabicki, M K Saravanan, Sarah Zennou, Daniel Bourdrez, Jason Noll, Ilias Cherkaoui, Felipe De Lima, Raul Siles, Matteo Bocchi, John Woods, Kostas Chalkias, Yolan Romailler, Gerardo Di Giacomo, Gregory Nazario, Rob Stubbs, Ján Jančár, Gabe Pike, Kiran Tummala, Stephen Singam, Jeremy O'Donoghue, Jeremy Boone, Thomas Duboucher, Charles Guillemet, Ryan Sleevi, Lionel Rivière, Benjamin Larsen, Gabriel Giono, Daan Sprenkels, Andreas Krogen, Vadim Lyubashevsky, Samuel Neves, Steven (Dongze) Yue, Tony Patti, Graham Steel, and all the livebook commenters for the many discussions and corrections, as well as technical and editorial feedback.

To all the reviewers: Adhir Ramjiawan, Al Pezewski, Al Rahimi, Alessandro Campeis, Bobby Lin, Chad Davis, David T Kerns, Domingo Salazar, Eddy Vluggen, Gábor László Hajba, Geert Van Laethem, Grzegorz Bernaś, Harald Kuhn, Hugo Durana, Jan Pieter Herweijer, Jeff Smith, Jim Karabatsos, Joel Kotarski, John Paraskevopoulos, Matt Van Winkle, Michal Rutka, Paul Grebenc, Richard Lebel, Ruslan Shevchenko, Sanjeev Jaiswal, Shawn P Bolan, Thomas Doylend, William Rudenmalm, your suggestions helped make this a better book.

about this book

It has now been more than two years since I've started writing *Real-World Cryptography*. I originally intended for it to be an introduction to all there is to know about the type of cryptography that is used in the real world. But, of course, that's an impossible task. No field can be summarized in a single book. For this reason, I had to strike a balance between how much detail I wanted to give the reader and how much area I wanted to cover. I hope you find yourself in the same box I ended up wiggling myself into. If you're looking for a practical book that teaches you the cryptography that companies and products implement and use, and if you're curious about how real-world cryptography works underneath the surface but aren't looking for a reference book with all the implementation details, then this book is for you.

Who should read this book

Here is a list of what I believe are the types of people (although please don't let anyone put you in a box) that would benefit from this book.

Students

If you're studying computer science, security, or cryptography and want to learn about cryptography as used in the real world (because you are either targeting a job in the industry or want to work on applied subjects in academia), then I believe this is the textbook for you. Why? Because, as I said in the preface, I was once such a student, and I wrote the book I wish I had then.

Security practitioners

Pentesters, security consultants, security engineers, security architects, and other security roles comprised most of the students I had when I taught applied cryptography. Due to this, this material has been refined by the many questions I received while I was trying to explain complicated cryptography concepts to non-cryptographers. As a security practitioner myself, this book is also shaped by the cryptography I've audited for large companies and the bugs that I learned about or found along the way.

Developers who use cryptography directly or indirectly

This work has also been shaped by the many discussions I've had with clients and coworkers, who were by and large neither security practitioners nor cryptographers. Today, it's becoming harder and harder to write code without touching cryptography, and as such, you need to have some understanding of what you're using. This book gives you that understanding using coding examples in different programming languages and more if you're curious.

Cryptographers curious about other fields

This book is an introduction to applied cryptography that's useful to people like me. I wrote this first to myself, remember. If I managed to do a good job, a theoretical cryptographer should be able to get a quick understanding of what the applied cryptography world looks like; another one working on symmetric encryption should be able to swiftly pick up on password-authenticated key exchanges by reading the relevant chapter; a third one working with protocols should be able to rapidly get a good understanding of quantum cryptography; and so on.

Engineering and product managers who want to understand more

This book also attempts to answer questions that I find to be more product-oriented: what are the tradeoffs and limitations of these approaches? What risk am I getting into? Would this path help me comply with regulations? Do I need to do this and that to work with a government?

Curious people who want to know what real-world crypto is about

You don't need to be any of the previous types I've listed to read this book. You just need to be curious about cryptography as used in the real world. Keep in mind, I don't teach the history of cryptography, and I don't teach the basics of computer science, so at the very least, you should have heard of cryptography before getting into a book like this one.

Assumed knowledge, the long version

What will you need in order to get the most out of this book? You should know that this book assumes that you have some basic understanding of how your laptop or the internet works, and at least, you should have heard of encryption. The book is about

real-world cryptography, and so it will be hard to put things in context if you're not at ease with computers or if you've never heard of the word *encryption* before.

Assuming that you somewhat know what you're getting into, it'll be a real plus if you know what bits and bytes are and if you've seen or even used bitwise operations like XOR, shift left, and those kinds of things. Is it a deal breaker if you haven't? No, but it might mean that you will have to stop for a few minutes here and there to do some Googling before you can resume reading.

Actually, no matter how qualified you are, when reading this book, you'll probably have to stop from time to time in order to get more information from the internet. Either because I (shame on me) forgot to define a term before using it or because I wrongly assumed you would know about it. In any case, this should not be a huge deal as I try to ELY5 (explain like you're 5) as best as I can the different concepts that I introduce.

Finally, when I use the word *cryptography*, your brain is probably thinking about math. If, in addition to that thought, your face grimaced, then you'll be glad to know that you shouldn't worry too much about that. *Real-World Cryptography* is about teaching insights so that you gain an intuition about how it all works, and it attempts to avoid the mathy nitty-gritty when possible.

Of course, I'd be lying if I said that no math was involved in the making of this book. There's no teaching cryptography without math. So here's what I'll say: it helps if you have achieved a good level in mathematics, but if you haven't, it shouldn't prevent you from reading most of this book. Some chapters will be unfriendly to you unless you have a more advanced understanding of math, specifically the last chapters (14 and 15) on quantum cryptography and next-generation cryptography, but nothing is impossible, and you can get through those chapters with willpower and by Googling about matrix multiplications and other things you might not know about. If you decide to skip these, make sure you don't skip chapter 16, as it's the icing on top of the cake.

How this book is organized: A roadmap

Real-World Cryptography is split into two parts. The first part is meant to be read from the first page to the last and covers most of the ingredients of cryptography: the stuff you'll end up using like Lego to construct more complex systems and protocols.

- Chapter 1 is an introduction to real-world cryptography, giving you some idea of what you'll learn.
- Chapter 2 talks about hash functions, a fundamental algorithm of cryptography used to create unique identifiers from bytestrings.
- Chapter 3 talks about data authentication and how you can ensure that nobody modifies your messages.
- Chapter 4 talks about encryption, which allows two participants to hide their communications from observers.

- Chapter 5 introduces key exchanges, which allows you to negotiate a common secret with someone else interactively.
- Chapter 6 describes asymmetric encryption, which allows multiple people to encrypt messages to a single person.
- Chapter 7 talks about signatures, cryptographic equivalents of pen-and-paper signatures.
- Chapter 8 talks about randomness and how to manage your secrets.

The second part of this book contains the systems that are built out of these ingredients.

- Chapter 9 teaches you how encryption and authentication are used to secure connections between machines (via the SSL/TLS protocol).
- Chapter 10 describes end-to-end encryption, which is really about how people like you and I can trust one another.
- Chapter 11 shows how machines authenticate people and how people can help machines sync with one another.
- Chapter 12 introduces the nascent field of cryptocurrencies.
- Chapter 13 spotlights hardware cryptography, the devices that you can use to prevent your keys from being extracted.

There are two bonus chapters: chapter 14 on post-quantum cryptography and chapter 15 on next-generation cryptography. These two fields are starting to make their way into products and companies, either because they are getting more relevant or because they are becoming more practical and efficient. While I won't judge you if you skip these last two chapters, you do have to read through chapter 16 (final words) before placing this book back on a shelf. Chapter 16 summarizes the different challenges and the different lessons that a cryptography practitioner (meaning you, once you finish this book) has to keep in mind. As Spider-Man's Uncle Ben said, "With great power comes great responsibility."

About the code

This book contains many examples of source code both in numbered listings and in line with normal text. In both cases, source code is formatted in a `fixed-width font like this` to separate it from ordinary text. Sometimes code is also **`in bold`** to highlight code that has changed from previous steps in the chapter, such as when a new feature adds to an existing line of code.

In many cases, the original source code has been reformatted; we've added line breaks and reworked indentation to accommodate the available page space in the book. In rare cases, even this was not enough, and listings include line-continuation markers (➥). Additionally, comments in the source code have often been removed from the listings when the code is described in the text. Code annotations accompany many of the listings, highlighting important concepts.

liveBook discussion forum

Purchase of *Real-World Cryptography* includes free access to a private web forum run by Manning Publications where you can make comments about the book, ask technical questions, and receive help from the author and from other users. To access the forum, go to https://livebook.manning.com/book/real-world-cryptography/discussion. You can also learn more about Manning's forums and the rules of conduct at https://livebook.manning.com/discussion.

Manning's commitment to our readers is to provide a venue where a meaningful dialogue between individual readers and between readers and the author can take place. It is not a commitment to any specific amount of participation on the part of the author, whose contribution to the forum remains voluntary (and unpaid). We suggest you try asking the author some challenging questions lest his interest stray! The forum and the archives of previous discussions will be accessible from the publisher's website as long as the book is in print.

about the author

DAVID WONG is a senior cryptography engineer at O(1) Labs working on the Mina cryptocurrency. Prior to that, he was the security lead for the Diem (formally known as Libra) cryptocurrency at Novi, Facebook, and before that, a security consultant at the Cryptography Services practice of NCC Group. David is also the author of the book *Real-World Cryptography*.

During his career, David has taken part in several publicly funded open source audits, such as OpenSSL and Let's Encrypt. He has spoken at various conferences, including Black Hat and DEF CON, and has taught a recurring cryptography course at Black Hat. He has contributed to standards like TLS 1.3 and the Noise Protocol Framework. He has found vulnerabilities in many systems, including CVE-2016-3959 in the Golang standard library, CVE-2018-12404, CVE-2018-19608, CVE-2018-16868, CVE-2018-16869, and CVE-2018-16870 in various TLS libraries.

Among others, he is the author of the Disco protocol (www.discocrypto.com and www.embeddeddisco.com) and the Decentralized Application Security Project for smart contracts (www.dasp.co). His research includes cache attacks on RSA (http://cat.eyalro.net/), protocol based on QUIC (https://eprint.iacr.org/2019/028), timing attacks on ECDSA (https://eprint.iacr.org/2015/839), or backdoors in Diffie-Hellman (https://eprint.iacr.org/2016/644). You can see and read about him these days on his blog at www.cryptologie.net.

about the cover illustration

The figure on the cover of *Real-World Cryptography* is captioned "Indienne de quito," or Quito Indian. The illustration is taken from a collection of dress costumes from various countries by Jacques Grasset de Saint-Sauveur (1757–1810), titled *Costumes de Différents Pays*, published in France in 1797. Each illustration is finely drawn and colored by hand. The rich variety of Grasset de Saint-Sauveur's collection reminds us vividly of how culturally apart the world's towns and regions were just 200 years ago. Isolated from each other, people spoke different dialects and languages. In the streets or in the countryside, it was easy to identify where they lived and what their trade or station in life was just by their dress.

The way we dress has changed since then and the diversity by region, so rich at the time, has faded away. It is now hard to tell apart the inhabitants of different continents, let alone different towns, regions, or countries. Perhaps we have traded cultural diversity for a more varied personal life—certainly for a more varied and fast-paced technological life.

At a time when it is hard to tell one computer book from another, Manning celebrates the inventiveness and initiative of the computer business with book covers based on the rich diversity of regional life of two centuries ago, brought back to life by Grasset de Saint-Sauveur's pictures.